(12) UK Patent Application (19) GB (11) 2 355 522 (13) A

(43) Date of A Publication 25.04.2001

(21) Application No 9924761.1

(22) Date of Filing 19.10.1999

(51) INT CL[7]
G07D 7/00

(52) UK CL (Edition S)
G1A AA6 AA9 AG17 AMBX AR6 AR7 AT20 AT21 AT3

(56) Documents Cited
GB 2219855 A GB 2192275 A EP 0660277 A
WO 99/42959 A US 4547896 A

(58) Field of Search
UK CL (Edition Q) G1A AMBX AMHL
INT CL[6] B07C 5/342 , G07D 7/00
Online: WPI, EPODOC, JAPIO

(71) Applicant(s)
Innovative Technology Limited
(Incorporated in the United Kingdom)
Derker Street, OLDHAM, OL1 4EQ, United Kingdom

(72) Inventor(s)
John Bailey
Steve Lewis

(74) Agent and/or Address for Service
David Keltie Associates
12 New Fetter Lane, LONDON, EC4A 1AG,
United Kingdom

(54) Abstract Title
Improvements in verifying printed security substrates

(57) Verifying the authenticity of a printed security substrate (50), such as a banknote or a bank cheque in a banknote validator comprises measuring the spectral response of the substrate (50) and relating the results at two spaced apart wavelengths to determine a quantity representative of the authenticity of the substrate (50). The spectral response is measured by illuminating a first portion (24) of the substrate (50) with a light source (20, 22) having a "blue" (UV) component (49) and a "red" (IR) component (48), and measuring the intensities with sensors (26, 28) of the blue and red components (49, 48) once they have been reflected off and transmitted through the substrate (50). The measured blue and red component intensities for either the reflected or the transmitted light components are related to each other using a predetermined function (f), such as a ratio of the blue to the red intensities. The result of the function indicates the authenticity of the substrate (50).

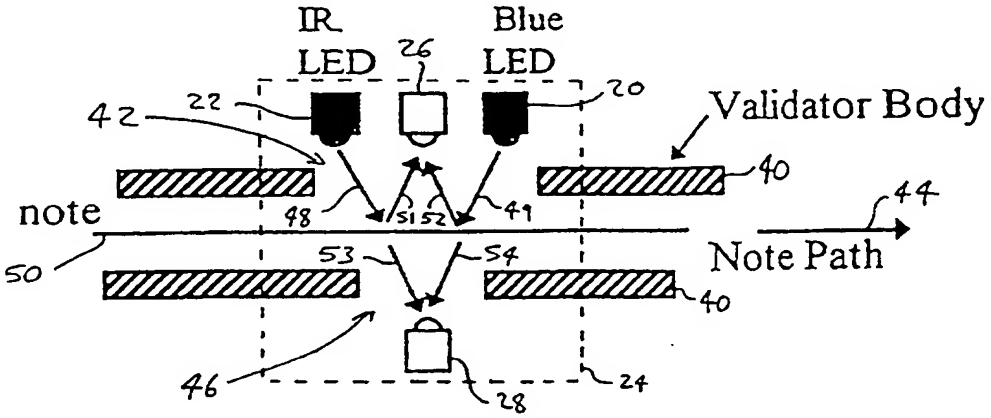

FIGURE 3

GB 2 355 522 A

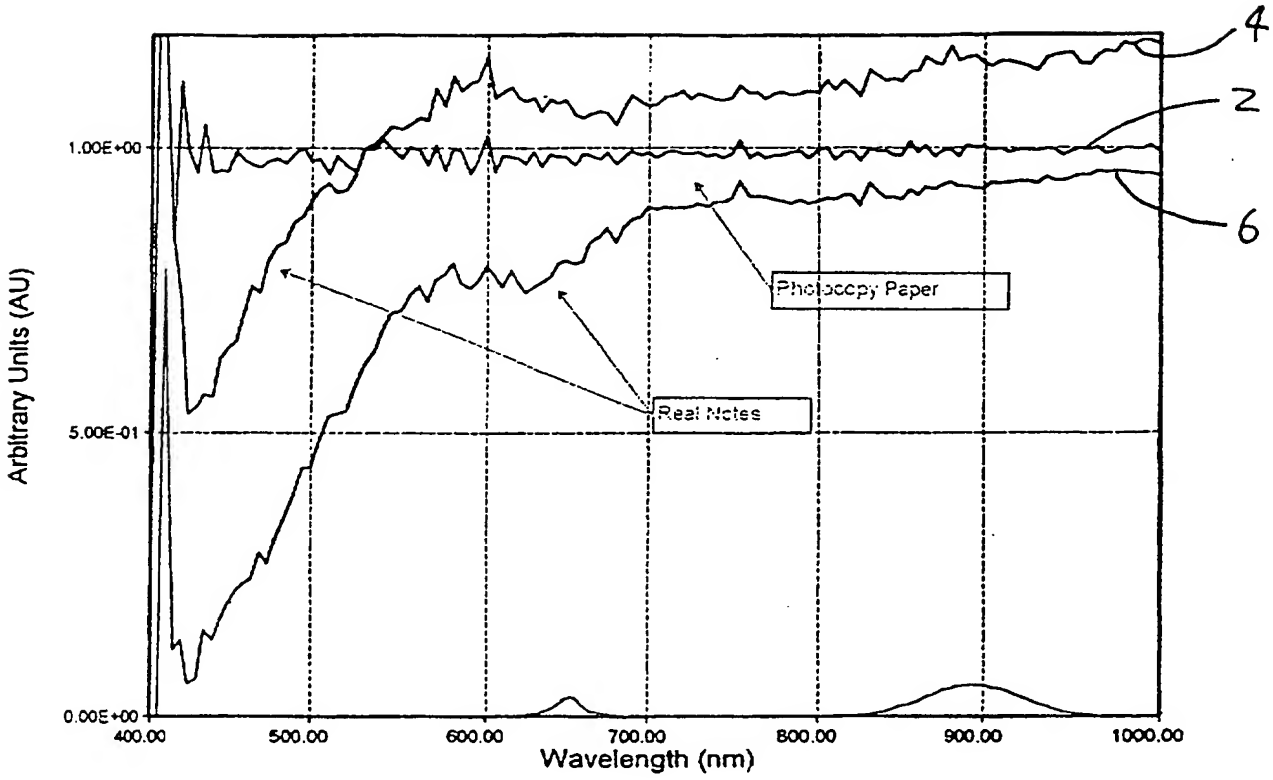
4
2
6
1.00E+00
5.00E-01
0.00E+00
Arbitrary Units (AU)
Photocopy Paper
Real Notes
400.00
500.00
600.00
700.00
800.00
900.00
1000.00
Wavelength (nm)

FIGURE 1

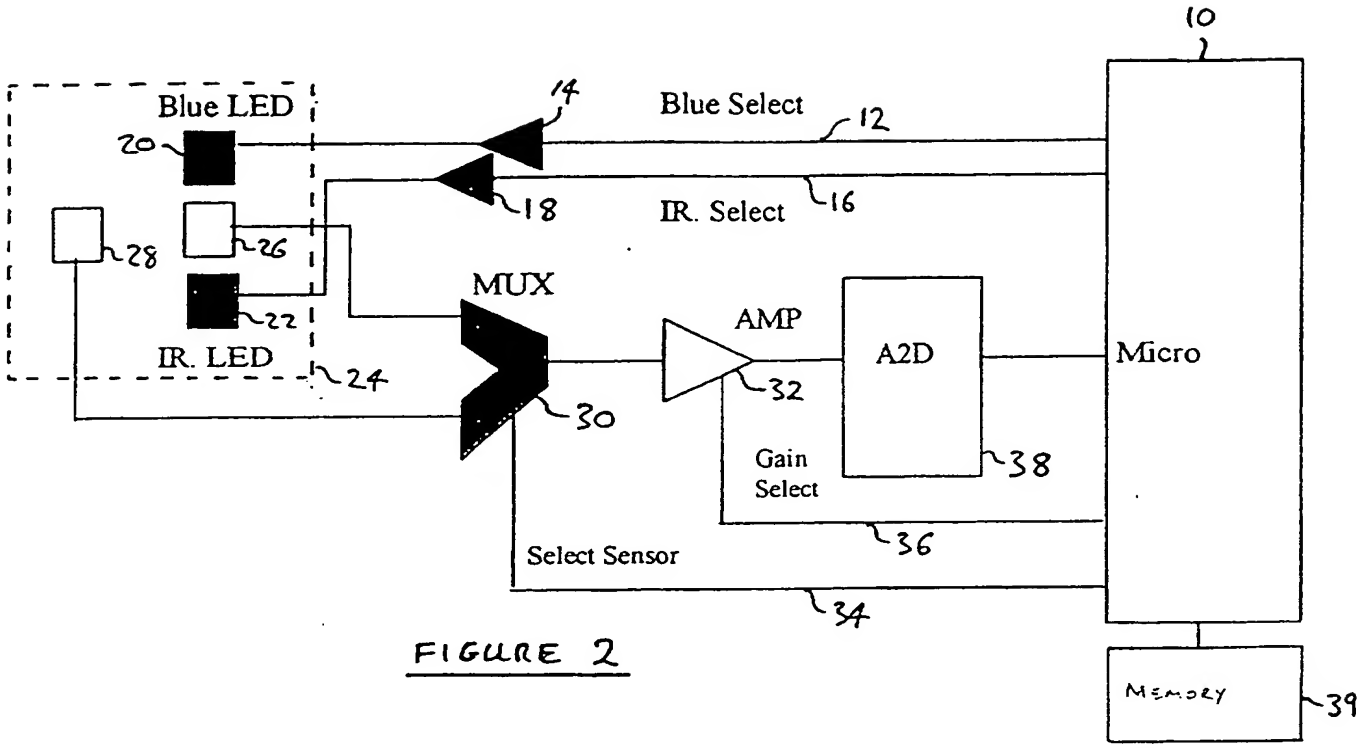

FIGURE 2

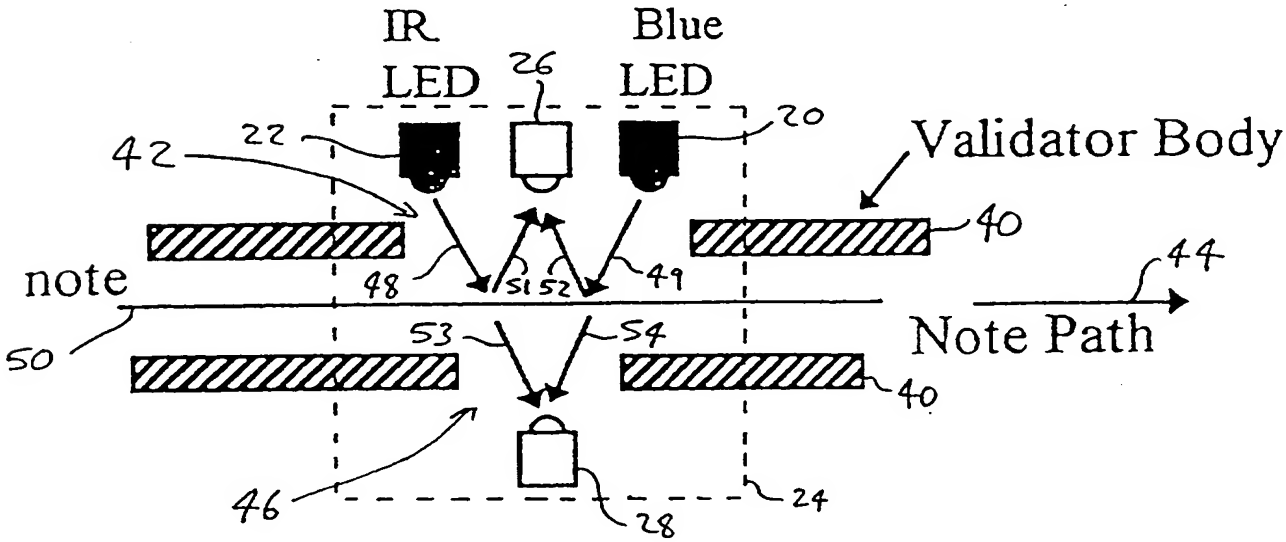

FIGURE 3

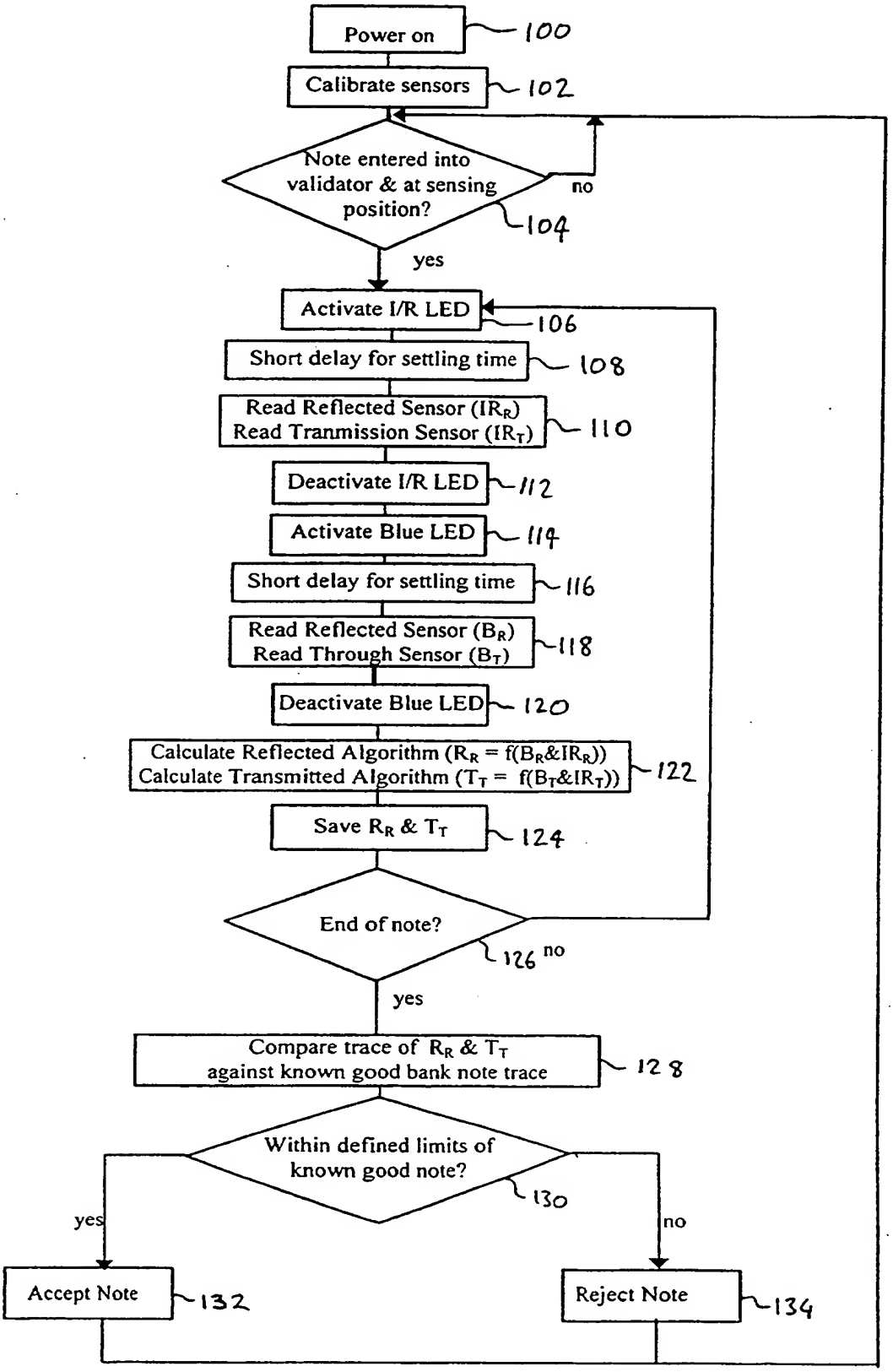

FIGURE 4

Improvements Relating to Verifying Printed Security Substrates

This invention concerns improvements relating to verifying printed security substrates and more particularly, though not exclusively, to a method of and an apparatus for verifying the authenticity of banknotes and cheques. The apparatus can be used as part of a banknote validator which accepts or rejects banknotes after checking for their authenticity.

The continually changing challenge for banknote validation companies is to keep up with the latest techniques used by counterfeiters to fool banknote validators. More particularly, as photocopier technology improves, positive discrimination, by banknote validators, between real banknotes and photocopied "samples" becomes an increasingly difficult problem. There are banknotes of several currencies, particularly those where the banknote has no areas of intense colour (e.g. 2000 ITL, 1000 GRD), which present significant challenges to the discrimination technology employed when black and white photocopies of them are presented to some existing validators.

Traditional methods of using fine tuning limits to accentuate the differences in response between the fake samples and the real banknote are time consuming and particularly with the above described types of banknotes do not work particularly well. Invariably, this adversely affects the acceptance levels of real banknotes.

Buried object (the silver line in the banknote) detection has helped the some banknote validators to reject these photocopies in the past, but recent experience with some UK fakes has shown that even this detection method can be fooled.

In regions such as the USA market, the banknotes (bills) are the same size and printed primarily in black. Also there are no buried objects on the one and two dollar bills. This makes differentiation, by means of colour sensors alone, between these banknotes and photocopies particularly difficult.

Several different tests are often used in the authentication of a banknote from photocopy forgeries. One of these presently used tests is to shine ultraviolet (UV) light on to the

banknote and to check its fluorescence levels. Most printed security substrates, such as banknotes, cheques, event tickets etc. are printed on high-quality non-fluorescent paper. This type of paper is not commonly available to the general public and is relatively expensive. Accordingly, most counterfeiters use conventional photocopier paper for their forgeries which fluoresces under UV light. This is because photocopy paper is impregnated with an optical brightner agent (OBA) which absorbs non-visible UV light present in normal daylight, and emits it at a higher wavelength in the visible region thereby making the paper appear brighter.

The fluorescence test has in the past been successful as part of a group of tests at determining photocopy counterfeits. However, in order to overcome this, counterfeiters have provided their counterfeit copies with a UV filter (by coating the copies with UV blocking agent) which prevents the counterfeit banknotes from fluorescing thereby giving the same result for the test as the genuine banknotes.

An object of the present invention is to overcome or substantially reduce these problems described above so as to provide an improved method of and apparatus for detecting fake security substrates such as banknotes.

The present invention resides in the appreciation that banknote paper and photocopier paper by their very composition have different spectral responses to light and that these spectral response differences are so significant that they can be used as the basis of a new robust discriminatory detection test.

More particularly, according to one aspect of the present invention there is provided a method of verifying the authenticity of a printed security substrate, the method comprising: illuminating a first portion of the substrate with a light source having a blue light component and a red light component; measuring the intensities of the blue and red light components once they have interacted with the substrate; and relating the measured blue and red light component intensities to each other using a predetermined function, such that the authenticity of the security substrate can be verified by the result of the relating step.

It is to be appreciated that the term printed security substrate has, in the context of the present invention, a broad meaning in that it covers any sheet-like objects having detectable features, for example banknotes, cheques, tickets and vouchers and fraudulent and counterfeit versions of the same. For the sake of convenience and ease of comprehension, the present invention is described in relation to the authentication of banknotes. However, the present invention is not so restricted and can be applied to the authentication of any printed security substrate.

The terms blue light component and red light component as used in the description of the present invention are not intended to be restricted to their strict literal meaning. Rather, it is to be appreciated that these terms simple indicate relative wavelengths between the components, the blue light component term being indicative of a relatively short wavelength light component and the red light component term being indicative of a relatively long wavelength light component. The wavelength of light covered by the blue light component can, for example, be recognised as a UV, green or yellow light. More specifically, the term blue light component is intended to represent wavelength in the electromagnetic spectrum of up to 570nm. Similarly, the term red light component is intended to mean a wavelength in the electromagnetic spectrum of 650nm and above.

The term relating as mentioned above, is intended to have a broad meaning in that it covers any way of comparing two quantities to determine a value representative of their relative difference. This can be realised in a simple way by use of a ratio of the two quantities or in a complex manner using a neural network for example.

The present invention as set out above is based around the inventors' discovery that the short wavelength spectral responses of an authentic security substrate is significantly different to that of a fake security substrate. Accordingly, regardless of the techniques used by the counterfeiters to imitate the printing on the security substrate, the method of the present invention determines the actual composition of the substrate, and so can even detect a flawless copy of a real banknote which has been printed on photocopier paper.

Unit to unit differences and temperature effects on the response of the individual sensors do not allow for the sensor means output to be used separately. However, when the blue sensor data is related to the infra-red data by some relationship, variations due to amplifier gain, offsets and temperature are minimised sufficiently to allow meaningful comparison between real security substrates and photocopied samples.

As mentioned previously, there are many different ways of relating the red and blue components together. Preferably, the predetermined function of the relating step comprises calculating a ratio of or a difference between the measured blue and red light component intensities. This is a simple (in terms of computing effort) low-cost way of achieving the relating step.

The measuring step may comprise measuring the reflection of the blue and red light components off a surface of the substrate. Alternatively or in addition, the measuring step may comprise measuring the transmission of the blue and red light components through the substrate. It was discovered through trials that some sample security substrates demonstrate this difference to the best advantage when the light is transmitted through the substrate and others when the light is reflected off the surface of the substrate. The use of either of these methods is sufficient to implement the present invention. However, there is a significant advantage if both techniques are used together in that a wider range of security substrates, each having different transmitted and reflected characteristics, can be detected.

Whilst there are many different ways of analysing the security substrates' spectral response, the full spectrum does not need to be measured. In an embodiment of the present invention, the illumination step comprises illuminating the first portion of the substrate with a blue light source and a red light source. Each of these different wavelength light sources enables the characteristics of the substrate to be measured at the specific wavelengths of the two light sources. Measuring the different responses at these two wavelengths is sufficient to fulfil the present invention and provides a relatively simple and low-cost way of measuring the required characteristics of the spectral response.

The blue light source preferably comprises an ultraviolet light source and the red light source preferably an infra-red light source. This difference between the wavelengths of the two light sources is important as it governs the diversity of substrates which can be authenticated without changing the method. Generally, as the difference between the wavelengths increases, the greater the number of different substrates which can be authenticated by the same method and the more robust it becomes.

Trials have shown that when the difference between the wavelengths is 100nm, then the difference between the red and blue component responses does not always provide sufficient reliability for the authentication method. Increasing the difference to 150nm has provided sufficiently different responses such that most different substrates can be authenticated reliably. Further increasing the difference to 200nm, ensures that the reliability of the method is sufficient for a commercial product with an acceptably low number of false rejections.

In an embodiment of the present invention, the illuminating step comprises two successive steps of illuminating the first portion of the substrate with the blue light component and illuminating the first portion of the substrate with the red light component. This advantageously provides a sufficient enough differentiation to enable a single sensor to be used for measuring both light components. Accordingly in this embodiment, the measuring step comprises measuring the intensities of the blue and red light components using a single sensor which has a large enough spectral response range to measure the wavelengths of light relating to both the blue and red light components.

Alternatively the illuminating step can comprise illuminating at least a portion of the substrate with both the blue and the red light components simultaneously. In this case, it is necessary to ensure that the measuring step comprises separating the measurement of the intensities of the blue and red light components. Separation can be achieved by measuring the light at successive time periods or by the measuring step comprising sensing the blue light component and the red light component using separate light sensors, each sensor being arranged to be sensitive to either of the blue or red light components.

Regardless of whether a single or different sensors are used, the sensor(s) can be made sensitive to the red or blue light components simply by use of appropriate wavelength light filters.

It is desirable to carry out the analysis of the substrate spectral response by considering the results at a portion substrate which is substantially free of printed matter, such as printing ink or buried objects. In order to increase the probability of finding such a portion of the substrate, the method preferably further comprises carrying out the illuminating, measuring and relating steps for a second portion of the security substrate, the second portion being spaced apart from the first portion. This doubles the area of the substrate being examined and also provides a back up means for implementing the method in the unlikely event of failure of the arrangement of sensors and light sources at the first portion of the substrate.

As a security substrate almost always has the same composition throughout, namely that it is usually made of one type of paper for example, it is only necessary to check the response of the substrate at a single point. However, as the presence of printing inks for example, can distort the results, it is advantageous to check several portions of the substrate. Accordingly, the method preferably further comprises repeating the illuminating, measuring and relating steps for a series of portions of the substrate as the same is passed through an illuminating and sensing position where the illuminating and sensing steps occur. In addition, some counterfeit banknotes are made up of substrate portions having different compositions. Another advantage of checking several portions of the substrate is to detect those substrate portions having counterfeit compositions. Clearly as the number of the substrate portions of the banknote that are checked increases, the better the method is at detecting fake banknotes. However, the economics of implementing increasing numbers of checks may restrict the actual number of checks to be carried out in practice.

If a single portion of the substrate is analysed, the method may further comprise verifying the authenticity of the substrate if the result of the relating step is above a predetermined threshold or within a predetermined set of limits. However, if the illuminating, measuring

and relating steps are repeated, then the method preferably further comprises selecting one of the results of the relating steps having a peak value for comparison with an associated predetermined threshold or with an associated predetermined set of limits and verifying the authenticity of the substrate if the selected result is above the threshold or within the set of limits.

An alternative way of verifying the authenticity of the security substrate where a series of portions of the substrate are analysed is for the method to further comprise creating a profile of the results of the relating steps and verifying the authenticity of the substrate if the profile is within predetermined profile limits.

Preferably, the selected result is chosen to represent a portion of the security substrate which is relatively free of printed images. These areas, as has been mentioned before, provide the most accurate representation of the nature of the substrate when analysed by the method of the present invention.

The method may further comprise storing a plurality of predetermined functions and associated threshold values and/or sets of limits and/or profile limits, each predetermined function and threshold value and/or set of limits and/or profile limits representing an optimum differentiating procedure for a specific type of substrate. In this way, the most appropriate way of carrying out the relating step can be implemented for a particular type of substrate.

The method preferably further comprises selecting a predetermined function and associated threshold value and/or set of limits and/or profile limits from the plurality of stored functions and values. The advantage of this is that the method can be adapted for use with different types of substrates without undue effort. In the case of a banknote validator, use of the method with various different types of currency would be possible by simply selecting the appropriate software option in the validator.

According to another aspect of the present invention, there is provided a substrate validator for verifying the authenticity of a printed security substrate, the validator comprising: light source means having a blue light component and a red light component

for illuminating a first portion of the substrate; light sensor means for measuring the intensities of the blue and red light components once they have interacted with the substrate; and means for relating the measured blue and red light component intensities to each other using a predetermined function, such that the authenticity of the security substrate can be verified by the result of the predetermined function.

The light source means may comprise two light sources one for the blue light component and one for the red light component. This enables a single sensor to be used for both measurements because both different wavelength responses can be sensed at different times by appropriate selection of the light source.

Preferably the light source means comprises an infra-red light source for generating the red light component and/or the light source means comprises an ultraviolet light source for the blue light component. Use of these sources gives a sufficient enough difference between the selected measurement wavelengths to provide reliable results with many different types of security substrates.

Preferably, the light source means comprises high-intensity light emitting diodes. This is one of the most cost-effective ways of controllably illuminating the substrate for this analysis. In particular, the provision of ultra-violet light emitting diodes is particularly advantageous because of the huge cost savings and benefits which result from their use in comparison to use of other ultra-violet light sources.

In an embodiment of the present invention, the relating means comprises a microprocessor arranged to implement the predetermined function and to compare the result of the predetermined function with a predetermined threshold or a predetermined set of limits or predetermined profile limits. The implementation of the present invention using a microprocessor advantageously enables the present invention to be integrated into existing security substrate devices such as banknote validators, which already include a microprocessor, without additional processing hardware. The only additional hardware required is that of the additional light source means and light sensor means.

Advantageously, the microprocessor can also be arranged to control the light source means and the light sensor means, without the need for further dedicated hardware.

The substrate validator may also further comprise a data store and the microprocessor may be arranged to store a plurality of predetermined functions and associated threshold values and/or sets of limits and/or profile limits in the data store, each predetermined function and associated threshold value and/or set of limits and/or profile limits representing an optimum differentiating procedure for a specific type of substrate.

According to another aspect of the present invention, there is provided a method of verifying the authenticity of a printed security substrate, the method comprising: measuring a spectral response of the substrate to illumination of a portion thereof from a light source; relating measured blue and red component intensities of the spectral response to each other by use of a predetermined function, and verifying the authenticity of the substrate by the result of the predetermined function.

Presently preferred embodiments of the present invention will now be described by way of example with reference to the accompanying drawings. In the drawings:

Figure 1 is a comparative graph showing the spectral response of authentic non-fluorescent banknote paper against photocopier paper;

Figure 2 is a schematic block diagram showing a banknote verification sensing circuit embodying the present invention;

Figure 3 is a schematic cross-sectional view the sensor arrangement used in the banknote verification sensing circuit of Figure 2; and

Figure 4 is a flow diagram showing the operation of the banknote verification sensing circuit of Figure 2.

A detailed comparative analysis between banknote paper and photocopier paper has been carried out which forms the basis of the present invention and this is described in greater detail below.

The inventors have discovered that there is a real difference which can be used in the present invention to distinguish authentic banknote paper from photocopied fakes. The difference is based on the fact that photocopier paper is made up of course cellulose fibres bulked out with chalk ($CaCO_3$) as opposed to authentic banknote paper which comprises very fine cellulose fibres supplemented with Titanium Dioxide (TiO_2).

The inventors have analysed the electromagnetic absorption characteristics from photocopier paper and has compared these to the electromagnetic absorption characteristics from authentic banknote paper. This was carried out by shining white light through samples of each of the two different types of paper, and analysing the response using a photo-spectrometer. The results, which are shown graphically in Figure 1, illustrate that there are different relative absorption values at different wavelengths for the photocopier paper and authentic banknote paper.

More particularly, the measured light readings for standard photocopier paper were normalised to give line 2 which is an approximately constant reading of 1.00 across the entire spectrum. The measured light readings for various authentic banknote papers shown as results lines 4,6 were then compared to this normalised line 2.

From the graphical results in Figure 1, it can be seen that while the response of photocopier paper and banknote paper are similar at infra-red wavelengths (800nm to 1000nm) the response of authentic banknote paper is considerably reduced at the blue/ultra violet end of the spectrum (400nm to 500nm). This difference was consistently reproducible in all of the banknotes tested (though only two are shown in Figure 1) and gave significant enough results to provide the basis of a robust authentication test.

On more detailed analysis of Figure 1 and other results (not shown), the range of light wavelengths which can be used in this analysis to produce differentiating results has been determined as 650nm and above for the red light component and 570nm and below for

the blue light component. When the difference between the red and blue light component wavelengths is selected to be 100nm, then the difference between the red and blue component responses does not always provide sufficient reliability for the authentication method. Increasing the difference to 150nm has provided sufficiently different response such that most different banknotes can be authenticated reliably. Increasing the difference to 200nm and more, ensures that the reliability of the method is sufficient for a commercial product with an acceptably low number of false rejections.

A preferred embodiment of the present invention is now described. The embodiment comprises a banknote validator circuit which is integrated into an existing banknote validator such as that described in International patent application WO-A-99/42959. For a detailed description of the existing banknote validator, the reader is referred to the above published patent application.

Referring now to Figure 2, a banknote validator circuit according to a presently preferred embodiment of the present invention is now described. The circuit comprises a microprocessor 10 which is arranged to output control signals and to receive a measurement reading. The microprocessor 10 is connected via a blue select line 12 to a blue LED driver circuit 14 and via an infra-red select line 16 to an infra-red LED driver circuit 18. The driver circuits 14,18 are simply analogue transistor drivers which directly interface to the microprocessor 10. The outputs of the blue and infra-red driver circuits 14,18 are respectively connected to an ultra-bright blue LED 20 and an infra-red LED 22 provided in an illumination and sensing region 24.

In use, the microprocessor 10 activates the blue and infra-red select lines 12,16 alternatively, such that the blue and infra-red select lines 12,16 are never both activated at the same time. This in turn ensures that the blue and red LEDs are activated alternately to generate blue and then infra-red illumination.

Two light sensors 26,28 are also provided in the illumination and sensing region 24. One light sensor 26 is positioned to sense reflected light from a banknote (see Figure 3) being authenticated and the other sensor 28 to sense light transmitted through the banknote. Both of the light sensors 26,28 have a spectral response range which is broad enough to

extend into both the infra-red and blue regions of the light spectrum. The outputs of the reflected light sensor 26 and the transmitted light sensor 28 are connected to a multiplexer 30 which acts to select either of these signals to output to an amplifier 32 where the selected signal is amplified. The selection of the sensor output at the multiplexer 30 and the gain setting of the amplifier 32 are controlled by the microprocessor 10 via a select sensor line 34 and a gain select line 36.

The selected sensor output, which has been amplified, is then converted from an analogue signal into a digital one at the A/D converter 38. The digital representation of the sensor signal is then passed onto the microprocessor 10 for use in a verification algorithm being implemented in the microprocessor 10. Digital representations of sensor signals from both the light sensors 26,28 are recorded for both the red and blue light stimuli thereby providing four results for a particular portion of the banknote.

The verification algorithm and the digital representations of the sensor signals are stored in a memory 39 connected to the microprocessor 10.

The arrangement of the LEDs 20,22 and sensors 26,28 in the illumination and sensing region 24 is now described in greater detail with reference to Figure 3.

Figure 3 shows how the LEDs 20,22 and sensors 26,28 are positioned in relation to a validator body 40. More particularly, the LEDs 20, 22 and the reflectance sensor 26 are provided at a reflection window 42 in the validator body 40 at one side of a note path 44. The transmitted light sensor 28 is provided at a transmission window 46 in the validator body 40 on the opposite side of the note path 44. The LEDs 20,22 and sensors 26,28 are all directed towards the note path 44.

When the LEDs 20,22 emit incident infra-red and blue light rays 48, 49 to illuminate a banknote 50 positioned between the windows 42,46 on the note path 44, some of the incident infra-red light rays 48 are reflected off the banknote 50 as infra-red light rays 51 to the reflected light sensor 26. Also, some of the incident blue light rays 49 are reflected back as blue light rays 52 to the reflected light sensor 26. In addition, some of the incident infra-red and blue light rays 48,49 are transmitted through the banknote 50 as

infra-red and blue light rays 53,54 to the transmitted light sensor 28. The sensors 26,28 are illuminated separately by infra-red light and blue light as has been mentioned previously. In this way, analogue measurements of the reflected and transmitted responses for both blue and infra-red light excitation of the banknote 50 can be recorded.

It is to be appreciated that whilst Figures 2 and 3 only show one set of LEDs 20,22 and sensors 26,28, in the presently preferred embodiment of the present invention there are two sets of such LEDs and sensors provided in two spaced-apart illumination and sensing regions (not shown). The additional set of LEDs and sensors is arranged to illuminate and measure a spectral response of a second illumination and sensing region of the banknote 50, to increase the portions of the banknote 50 being analysed at any one time. The additional set is connected up to the microprocessor 10 in a similar manner to that of the first set.

A method of authenticating a banknote according to an embodiment of the present invention is now described using the circuit described above. A banknote 50 is fed into a banknote validator (not shown) along the note path 44. When the banknote reaches the illumination and sensing region 24, the infra-red LED 22 and the blue LED are flashed at the banknote 50 alternately. The reflected and transmitted light rays 51,52,53,54 are measured for each of the infra-red and blue illuminations and the results are collated in the memory 39 via the microprocessor 10. This process carries on continuously whilst the banknote 50 is travelling through the illumination and sensing region 24 with the results being stored in the memory 39 via the microprocessor 10.

Once the banknote 50 has passed through the illumination and sensing region 24, the stored raw data regarding reflected and transmitted light for each infra-red and blue flash illumination is analysed by the algorithm running on the microprocessor 10. There are three possible ways of processing the data to determine its authenticity and these are set our below:

1) the raw data is converted into a results profile using a predetermined function which relates the blue light sensor results to the red light sensor results. Such functions are described in detail below. The results profile is then compared to that of a genuine

banknote and if the results profile is outside predetermined limits (tolerance limits) of the profile for the genuine banknote then the banknote is rejected as being a forgery;

2) the raw data is collected and processed in an attempt to determine those samples which give the best results. In the present case, some of the best results for differentiating photocopier paper from authentic banknote paper are obtained from the results calculated for an area of the banknote which has a minimal amount of printing ink and which is preferably free from printing inks altogether. This type of area gives, in terms of the authentication test, one of the best representations of the characteristics of the banknote substrate itself. The raw data for all the samples is processed by a predetermined function (described in detail below) which relates the blue light sensor results to the red light sensor results. Those results which give the largest values are selected for further analysis. These largest values are then compared to the results of a genuine banknote at corresponding locations and if the result is outside predetermined set limits (tolerance limits) for the genuine banknote then the banknote is rejected as being a forgery; and

3) the procedure is exactly the same as in the second way of processing the raw data except that the selected results of the function are compared to that of a genuine banknote and if the result is below a predetermined minimum threshold for the genuine banknote then the banknote is rejected as being a forgery.

It is to be appreciated that it is not essential that the raw data is stored at all. The above three ways can be adapted to implement the predetermined function on the data as it is generated and to store only the results of the function in the memory 39. This reduces the size of the memory required. Furthermore, the memory can be used to store all of the different methods described above. Different thresholds, tolerance limits and profile limits for different types of banknotes could also be stored such that the validator can operate with different currencies. In these cases, the user can select in software the most appropriate type of method and its associated thresholds or limits for a particular desired application.

Referring to Figure 4, a method of operating the above described circuit is now described in detail with reference to the first described possible ways of processing the data to determine its authenticity. The method is effectively an algorithm which is implemented on the microprocessor 10.

The method commences at 100 with the banknote validator being switched on. The first processing step occurs at 102 with the calibration of each of the sensors of the validator. Calibration techniques are well known and are not described hereinafter.

The algorithm running on the microprocessor 10, then checks at 104 whether a banknote 50 has been entered into the validator. More specifically a check is made to determine whether a banknote has been entered and if it has, whether it has reached the illumination and sensing position 24. If the answer is no, then the check is repeated. If the answer is yes, then the illumination and sensing steps are activated. These steps commence with the infra-red LED 22 being activated at 106 by a control signal from the microprocessor 10. This is followed by a short delay of 100μS at 108 allowing for the electronics to settle. Then the readings of the reflected light sensor 26 and the transmitted light sensor 28 are taken at 110 and their digital representations (IR_R and IR_T respectively) are stored in the memory 39. The infra-red LED 22 is then deactivated at 112.

The above described process is then repeated for the blue LED 20. This commences at 114 with the blue LED 20 being activated. Following the subsequent 100μS delay at 116, the reflected light sensor 26 and the transmitted light sensor 28 are both read at 118 and the digitised readings (B_R and B_T respectively) are stored in the memory 39. Then the blue LED is deactivated at 120 from the microprocessor 10.

Clearly there is movement of the banknote between the red and the blue light sensor readings. However, it is not essential for the red and blue light readings to be of exactly the same portion of the banknote 50 and this movement is very small in the time period between the sensor readings. Also the signal noise generated by the movement is negligible and so there is no difficulty in taking the readings of a moving banknote.

Using the stored digitised results, a reflection result (R_R) and a transmission result (T_T) are calculated using blue and infra-red readings for each of the reflected and transmitted signals as set out below:

$$R_R = f(B_R \,\&\, IR_R)$$
$$T_T = f(B_T \,\&\, IR_T)$$

where f (a,b) is a predetermined function relating a and b together.

In the present embodiment, the relationship used is to divide the infra-red reading by the blue reading for both reflected and transmitted light sensors,

i.e. $\frac{\text{Infra-red (Transmitted)}}{\text{Blue (Transmitted)}}$ & $\frac{\text{Infra-red (Reflected)}}{\text{Blue (Reflected)}}$

Which gives:

$$R_R = IR_R / B_R$$
$$T_T = IR_T / B_T$$

The calculated values of R_R and T_T are saved at 124 in the memory 39. Then the sensors 26,28 at the illumination and sensing position 24 are checked at 126 to determine where the end of the banknote 50 has been reached. If there is another portion of the banknote 50 which could be analysed, then the above steps 106 to 126 are repeated for the new part of the banknote 50. Otherwise, if it is the end of the banknote 50, then all the required readings from the banknote 50 will have been taken and a series of calculated values of R_R and T_T (profile or trace) of reflected results and transmitted results will be available.

The next step in this verification of the banknote is for the trace of the reflected results and the trace of the transmitted results to be compared at 128 with those of an authentic banknote 50. If both the measured traces are at 130 within predefined tolerance limits then the banknote 50 is accepted at 132. Otherwise, as at least one of the measured traces is outside the tolerance limits, the banknote is rejected at 134. In this case, the false banknote is rejected and returned to the user. The algorithm then awaits at 104 the entry of the next banknote 50 into the validator.

Other ways of relating the measured components together can also be used. These other relationships are still based on a comparison the measured infra-red component and the blue component and these can be used in alternative embodiments of the present invention. For example, some other exemplary relationships are set out below:

1. $\frac{\text{Blue (Transmitted)}}{\text{Infra Red (Transmitted)}}$ & $\frac{\text{Blue (Reflected)}}{\text{Infra Red (Reflected)}}$

Which gives:

$$R_R = B_R / IR_R$$
$$T_T = B_T / IR_T$$

2. Blue (Transmitted) - Infra Red (Transmitted) & Blue (Reflected) - Infra Red (Reflected)

Which gives:

$$R_R = B_R - IR_R$$
$$T_T = B_T - IR_T$$

3. $\frac{\text{Blue (Transmitted) - Infra Red (Transmitted)}}{\text{Infra Red (Transmitted)}}$ & $\frac{\text{Blue (Reflected) - Infra Red (Reflected)}}{\text{Infra Red (Reflected)}}$

Which gives:

$$R_R = (B_R - IR_R) / IR_R$$
$$T_T = (B_T - IR_T) / IR_T$$

4. $\frac{\text{Blue (Transmitted) - Infra Red (Transmitted)}}{\text{Blue (Transmitted)}}$ & $\frac{\text{Blue (Reflected) - Infra Red (Reflected)}}{\text{Blue (Reflected)}}$

Which gives:

$$R_R = (B_R - IR_R) / B_R$$
$$T_T = (B_T - IR_T) / B_T$$

Furthermore, the comparisons could be carried out by the use of neural networks or other multivariate statistical techniques. These techniques are not described herein because they are well understood by those of appropriate skill in the art.

Currently most UV sources are not of a sufficiently low price to be included within a low cost validator. However, a recent development of ultraviolet LEDs means that a UV light source can be incorporated into the circuit at lost cost.

The above embodiment has been described using a continuously moving banknote 50. However, it would also be possible to have the banknote stopping intermittently for each

sensor reading to be taken. Whilst the entire process would slow down, this would reduce background signal noise associated with the banknote movement, and would be useful in noisy environments.

It would also be possible to have a single elongate illumination and sensing region rather than two spaced-apart discrete illumination and sensing regions. In this case, each LED light source in the above embodiment could be replaced by a strip (array) of appropriately coloured LEDs and each sensor by a strip (array) of appropriately positioned sensors. The advantage of this arrangement would be that the authentication process would be even more robust in that there would be no need to provide banknote positional alignment with the sensors. Positional alignment is sometime required with validators when fine tuning tubes are being used for banknote discrimination and validation.

In this case, the method would further comprise collating the results from all of the sensors in the strip, applying the above described algorithm to the results and then analysing the results to select the largest (peak) values for comparison with predetermined limits or a minimum threshold as set out in the above described second and third ways of processing the raw data. In other words, the methods employed in analysing data collected along the length of a banknote would be applied in analysing the banknote across its width. Alternatively, fine tuning limits could be used on all of the results of the data collected across the width of the banknote.

In an alternative embodiment, the infra-red and blue LEDs could be provided by a single multi-coloured (white) light source or by a red, a green and a blue LED all being driven simultaneously. In this case, each of the reflected light and transmitted light sensors could be replaced by two sensors, one with an infra-red light biased spectral response and one with a blue-light biased spectral response. The biasing of each of these four sensors could be achieved by simply providing an appropriate infra-red or blue filter with each of the sensors. Preferably, the red filter would only pass light having a wavelength above 650nm with the blue filter only passing light at least 150nm below this wavelength or the blue filter would only pass light having a wavelength below 570nm with the red filter passing light at least 150nm above this wavelength. In practice, the greater the spacing between the these cut-off wavelengths the better the authentication process becomes.

Alternatively, the biasing could be achieved by appropriate selection of sensors with peak spectral responses shifted towards the red or blue ends of the light spectrum. The advantage of such an arrangement would be that no intermediate pulsing of the light sources would be required though the greater number of components would increase costs.

Having described particular preferred embodiments of the present invention, it is to be appreciated that the embodiments in question are exemplary only and that variations and modifications such as will occur to those possessed of the appropriate knowledge and skills may be made without departure from the spirit and scope of the invention as set forth in the appended claims.

CLAIMS:

1. A method of verifying the authenticity of a printed security substrate, the method comprising:

illuminating a first portion of the substrate with a light source having a blue light component and a red light component;

measuring the intensities of the blue and red light components once they have interacted with the substrate; and

relating the measured blue and red light component intensities to each other using a predetermined function, such that the authenticity of the security substrate can be verified by the result of the relating step.

2. A method according to Claim 1, wherein the predetermined function of the relating step comprises calculating a ratio of the measured blue and red light component intensities.

3. A method according to Claim 1 or 2, wherein the predetermined function of the relating step comprises calculating a difference between the measured blue and red light component intensities.

4. A method according to any preceding claim, wherein the measuring step comprises measuring the reflection of the blue and red light components off a surface of the substrate.

5. A method according to any preceding claim, wherein the measuring step comprises measuring the transmission of the blue and red light components through the substrate.

6. A method according to any preceding claim, wherein the illumination step comprises illuminating the first portion of the substrate with a blue light source and a red light source.

7. A method according to Claim 6, wherein the blue light source comprises an ultraviolet light source.

8. A method according to Claim 6 or 7, wherein the red light source comprises an infra-red light source.

9. A method according to any preceding claim, wherein the illuminating step comprises two successive steps of illuminating the first portion of the substrate with the blue light component and illuminating the first portion of the substrate with the red light component.

10. A method according to Claim 9, wherein the measuring step comprises measuring the intensities of the blue and red light components using a single sensor which has a large enough spectral response range to measure the wavelengths of light relating to both the blue and red light components.

11. A method according to any of Claims 1 to 8, wherein the illuminating step comprises illuminating at least a portion of the substrate with both the blue and the red light components simultaneously.

12. A method according to any preceding claim, wherein the measuring step comprises separating the measurement of the intensities of the blue and red light components.

13. A method according to Claim 12 as dependant on any of Claims 1 to 9 and 11, wherein the measuring step comprises sensing the blue light component and the red light component using separate light sensors, each sensor being arranged to be sensitive to either of the blue or red light components.

14. A method according to Claim 13, wherein the sensors are sensitive to the red or blue light components by use of appropriate wavelength light filters.

15. A method according to any preceding claim, further comprising carrying out the illuminating, measuring and relating steps for a second portion of the security substrate, the second portion being spaced apart from the first portion.

16. A method according to Claim 15, wherein the illuminating step comprises illuminating a plurality of portions of the substrate forming a strip portion across the security substrate and the measuring step comprises measuring the blue and red light components which have interacted with the substrate at each of the plurality of portions which comprise the strip portion.

17. A method according to Claim 16, wherein the illuminating, measuring and relating steps are carried out for each of the plurality of portions comprising the strip portion and the method further comprises selecting the results of the relating steps having a peak value for further analysis.

18. A method according to any preceding claim, further comprising verifying the authenticity of the substrate if the result or results of the relating step or steps is above a predetermined threshold.

19. A method according to any of Claims 1 to 18, further comprising verifying the authenticity of the substrate if the result of the relating step is within a predetermined set of limits.

20. A method according to any of Claims 1 to 17, further comprising repeating the illuminating, measuring and relating steps for a series of portions of the substrate as the same is passed through an illuminating and sensing position where the illuminating and sensing steps occur.

21. A method according to Claim 20, further comprising selecting one of the results of the relating steps having a peak value for comparison with an associated predetermined threshold and verifying the authenticity of the substrate if the selected result is above the threshold.

22. A method according to Claim 20, further comprising selecting one of the results of the relating steps having a peak value for comparison with an associated predetermined

set of limits and verifying the authenticity of the substrate if the selected result is within the set of limits.

23. A method according to Claim 20, further comprising creating a profile of the results of the relating steps and verifying the authenticity of the substrate if the profile is within predetermined profile limits.

24. A method according to Claim 21 or 22, wherein the selected result is chosen to represent a portion of the security substrate which is relatively free of printed images.

25. A method according to any preceding claim, further comprising storing a plurality of predetermined functions and associated threshold values and/or sets of limits and/or profile limits, each predetermined function and threshold value and/or set of limits and/or profile limits representing an optimum differentiating procedure for a specific type of substrate.

26. A method according to Claim 25, further comprises selecting a predetermined function and associated threshold value and/or set of limits and/or profile limits from the plurality of stored functions and values.

27. A method according to any preceding claim, wherein the respective wavelengths of the red and blue components are at least 150 nm apart.

28. A method according to any of Claims 1 to 26, wherein the respective wavelengths of the red and blue components are at least 200 nm apart.

29. A substrate validator for verifying the authenticity of a printed security substrate, the validator comprising:

light source means having a blue light component and a red light component for illuminating a first portion of the substrate;

light sensor means for measuring the intensities of the blue and red light components once they have interacted with the substrate; and

means for relating the measured blue and red light component intensities to each other using a predetermined function, such that the authenticity of the security substrate can be verified by the result of the predetermined function.

30. A substrate validator according to Claim 29, wherein the light source means comprises a blue light source and a red light source.

31. A substrate validator according to Claim 29 or 30, wherein the light source means comprises an infra-red light source.

32. A substrate validator according to any of Claims 29 to 31, wherein the light source means comprises an ultraviolet light source.

33. A substrate validator according to any of Claims 29 to 32, wherein the light source means comprises high-intensity light emitting diodes.

34. A substrate validator according to any of Claims 29 to 33, wherein the light sensor means comprises a light sensor arranged in relation to the substrate and the light source means to sense blue and red light components reflected off a surface of the substrate.

35. A substrate validator according to any of Claims 29 to 34, wherein the light sensor means comprises a light sensor arranged in relation to the substrate and the light source means to sense blue and red light components transmitted through the substrate.

36. A substrate validator according to any of Claims 29 to 35, wherein the light sensor means has a wide-band spectral response which maximises the range of wavelengths which can be detected.

37. A substrate validator according to any of Claims 29 to 36, wherein the relating means comprises a microprocessor arranged to implement the predetermined function and to compare the result of the predetermined function with a predetermined threshold or a predetermined set of limits or predetermined profile limits.

38. A substrate validator according to Claim 37, wherein the microprocessor is also arranged to control the light source means and the light sensor means.

39. A substrate validator according to Claim 37 or 38, further comprising a data store and wherein the microprocessor is arranged to store a plurality of predetermined functions and associated threshold values and/or sets of limits and/or profile limits in the data store, each predetermined function and associated threshold value and/or set of limits and/or profile limits representing an optimum differentiating procedure for a specific type of substrate.

40. A substrate validator according to any of Claims 29 to 39, further comprising a further light source means, a further light sensor means and a further relating means arranged to illuminate and measure a spectral response of a second portion of the security substrate, the second portion being spaced apart from the first portion.

41. A substrate validator according to any of Claims 20 to 40, further comprising a plurality of light source means arranged in an array and a plurality of light sensors arranged in a corresponding array.

42. A substrate validator according to any of Claims 29 to 41, wherein the wavelength of the red and the blue light components are at least 150nm apart.

43. A substrate validator according to any of Claims 29 to 42, wherein the wavelength of the red and the blue light components are at least 200nm apart.

44. A method of verifying the authenticity of a printed security substrate, the method comprising: measuring a spectral response of the substrate to illumination of a portion thereof from a light source; relating measured blue and red component intensities of the spectral response to each other by use of a predetermined function, and verifying the authenticity of the substrate by the result of the predetermined function.

45. A method substantially as described herein with reference to Figure 4 of the accompanying drawings.

46. A substrate validator substantially as described herein with reference to Figures 2 and 3 of the accompanying drawings.

The Patent Office

27

INVESTOR IN PEOPLE

Application No: GB 9924761.1
Claims searched: 1, 29, 44

Examiner: Simon Colcombe
Date of search: 20 December 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G1A (AMBX, AMHL)

Int Cl (Ed.6): G07D 7/00, 7/12 : B07C 5/342

Other: Online: WPI, EPODOC, JAPIO.

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2219855	(LAUREL) Abstract and page 14, lines 7-16.	1-6,8,11-23,25-27,29-31,33-35,37-39,41-44
X	GB 2192275	(LAUREL) Abstract	1-6,8,11-23,25-27,29-31,33-35,37-39,41-44
X	EP 0660277	(AZKOYEN) Page 3, lines 30 - 47, Fig 1.	1,4-8,10 11,12,25,26,29-39 44
X	WO 99/42959	(INNOVATIVE) Page 3, line 20- page 5, line 11	1,4-6,8,11-22,25,29,30,31,34-37,39,41,44
X	US 4547896	(OHTOMBE) Fig 3, Col 2, line 40 - col 3, line 65. Col 5, lines 20-30.	1-6,11-26,29,30,34,36,37,39 44

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.